Amendments to the Specification

Please replace the paragraph on page 11, beginning with line 8, with the following:

The architecture also includes a plurality of access modules 112 that are configured to enable a user to access the authentication/negotiation component 110. Although only one access module is shown for each authentication/negotiation component 110, more than one access module 112 can be provided for each authentication/negotiation component 110. Architecture 100 can also include a global authentication database 114 that is configured to be globally accessible from anywhere in the world. In the illustrated example, the global authentication database includes not only a repository of data or information that is used to authenticate users, but also any server computers or computing devices that are used in connection with the data repository to authenticate a user. The global authentication database 114 is advantageously accessible via the Internet 102. The global authentication database 114 can be any suitable globally accessible database that is capable of authenticating users as described below. Such databases can be operated by and/or associated with particular businesses, organizations or clubs for which authentication is desired. For example, a particular organization, e.g. Gold Club Frequent Fliers, may have negotiated with authentication/negotiation component 110 for Internet access for its members. When the members access the network ~~112~~ 104 through the access module 112, there needs to be a way to authenticate these Gold Club Frequent Flyer members so that they can be provided Internet access at the negotiated level. The global authentication database

114 provides a mechanism by which this can be done, as will become apparent below. Alternately, the global authentication database 114 can be a more generalized database that can be operated on behalf of many organizations or businesses that might want to generally authenticate users. An example of this type of global authentication database is the MICROSOFT® ~~Microsoft's~~ Passport Server and database. The MS server and database enable a user to be individually verified against information that is maintained by the server and database. Often times, this type of verification is conducted outside of the purview of other servers in an end-to-end secure fashion.

Please replace the paragraph on page 22, beginning with line 14, with the following:

The authentication/negotiation component 110a can also include (although it is not specifically shown) a dynamic host configuration protocol (DHCP) server that is responsible for issuing and managing IP addresses. DHCP servers are known and will not be further discussed herein. Alternatively, the authentication/negotiation component 110a can include a Network Address ~~Tranlator~~ Translator (NAT) software module. NAT is responsible for issuing private addresses to clients and then translating these to public routable IP addresses. NAT is also known and will not be further discussed herein.

Please replace the paragraph on page 22, beginning with line ~~14~~ 22, with the following:

In the illustrated example, a global authentication database 114a is provided in the form of the MICROSOFT® ~~Microsoft's~~ Passport Server. As pointed out above, any suitable global database can be used. This global authentication database 114a can comprise multiple different machines that are located globally around the world. The database is used, in one embodiment, to authenticate users as will be described in the "Authentication" section just below.

Please replace the paragraph on page 23, beginning with line 5, with the following:

Fig. 3b shows an alternate architecture in which the host organization subnet comprises a authentication/negotiation component 110b that includes a PANS Authorizer 302b and a policy manager 304a. The PANS Authorizer 302b authenticates users just as described above. In this particular architecture, the verification functionality is shifted to the access modules 112b in the form of a PANS verifier module 308 that resides at one or more of the access points of the access module. In the illustrated example, a PANS verifier 308 resides at each of the access points 306a. The advantages of providing a PANS verifier at each access point 306a include the detection of rogue users early on before they access the system. That is, once a user is authenticated, the PANS Authorizer 302b passes the verification function to the PANS verifier 308 at one or

more of the access points 306a. Thus, whenever a user attempts to send a data packet to the Internet, they are verified at the access module before the packet is transmitted to the authentication/negotiation component 110b. If a rogue user attempts to transmit an unauthorized packet, the packet can be detected very early in the architecture chain.

Please replace the paragraph on page 35, beginning with line 5, with the following:

Fig. 8 shows a flow diagram that describes steps in a quality of service method in accordance with the described embodiment. Some of the illustrated steps can be implemented by the PANS server 302, while other of the steps can be implemented by the client. Step 800 displays one or more service level options for a user. In the described embodiment, the service level options can be displayed on the client machine so that the user can select an appropriate level. For example, if a user is in a busy airport and is between flights, they may only have a limited amount of time to transacts their on line business. In this instance, the user may select the premium Level I service level so that they have the best chance of transacting their business. The service level options might also be displayed in the form of a list that describes various member organizations that have negotiated for particular service levels on behalf of their members. Step 802 selects a service level option. This step can be implemented by the user selecting a particular displayed service level. Alternately, the user can select from among the groups that are described in the list of member organizations. After the user has been authenticated,

step 804 monitors the data packet traffic that is generated from all of the users. Step 804 is typically a continuously implemented step in which the data packet traffic is monitored as users are added to and deleted from the collection of users that are transmitting data packets at any particular time. In this example, since all of the data packets from each of the users or clients gets routed through the PANS server, it is in the best position to oversee, monitor and control the packet flow. The PANS server then, in accordance with its programming instructions, generates a "go" signal (step 806) when a user or group of users is authorized to transmit their data packets. Steps 808 and 810 wait to receive the "go" signal. Once the "go" signal is received, if the authorized recipient is an individual user (step 812), then they can begin their data packet transmission (step 814). If the authorized recipient comprises a group of users (e.g. Level II or III users), they can begin their arbitration process (step 816).